IN THE CLAIMS

1. (Previously Presented) A method of secure information distribution between nodes, the method comprising:

providing, by a first node, a component value A1;

providing, by an adjacent node, a component value B1 as a challenge to the first node;

performing, by the first node, a handshake process with the adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to calculate identical values by applying the component values A1 and B1, and a key value associated with the secure group, to a one way function f(x); and

distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

2. (Original) The method of claim 1, further comprising:

prior to providing the secure information to the adjacent node, performing the handshake process with another adjacent node.

3. (Original) The method of claim 1, further comprising:

establishing an encryption key with the adjacent node.

4. (Original) The method of claim 3, wherein the encryption key comprises a public key.

5. (Original) The method of claim 3, wherein the encryption key comprises a symmetric key.

6. (Original) The method of claim 3, wherein the secure information is distributed along with an encryption key.

7-9. (Cancelled)

10. (Previously Presented) The method of claim 1, wherein the one way function f(x) is a secure hash function.

11. (Original) The method of claim 1, wherein the secure information comprises a password.

12 (Original) The method of claim 1, wherein the secure information comprises a key for secure communication.

13. (Original) The method of claim 1, further comprising:

distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

14. (Original) The method of claim 1, wherein the action of performing the handshake process comprises:

performing the handshake process with the adjacent node once for every fixed time amount T.

15. (Original) The method of claim 1, further comprising:

after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0).

16. (Original) The method of claim 1, further comprising:

determining an age of the secure information so that each node in the secure group will store a latest version of the secure information.

17. (Original) The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a sequence number of the secure information to determine the age of the secure information.

18. (Original) The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a date of modification of the secure information to determine the age of the secure information.

19. (Original) The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking an elapsed time since a previous modification of the secure information to determine the age of the secure information.

20. (Original) The method of claim 1, further comprising:

resolving an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value.

21. (Previously Presented) The method of claim 1, further comprising:

increasing a security of the secure group by widening the key value which is known by each node in the secure group.

22. (Original) The method of claim 1, further comprising:

decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

23. (Original) The method of claim 1, further comprising:

allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

24. (Original) The method of claim 1, further comprising:

preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

25. (Previously Presented) An apparatus for secure information distribution between nodes, the apparatus comprising:

a node configured to perform a handshake process with an adjacent node to determine membership in a secure group, and distribute secure information to the adjacent node, if the adjacent node is proven to be a member of the secure group;

wherein the handshake process comprises requiring each of the node and the adjacent node to calculate identical values by applying a component value A1 provided by the node, a component value B1 provided by the adjacent node, and a key value associated with the secure group, to a one way function f(x).

26. (Original) The apparatus of claim 25, wherein the node performs the handshake process with another adjacent node, prior to providing the secure information to the adjacent node.

27. (Original) The apparatus of claim 25, wherein the node is configured to establish an encryption key with the adjacent node.

28. (Original) The apparatus of claim 25, wherein the encryption key comprises a public key.

29. (Original) The apparatus of claim 25, wherein the encryption key comprises a symmetric key.

30. (Original) The apparatus of claim 27, wherein the secure information is distributed along with an encryption key.

31. (Cancelled)

32. (Previously Presented) The apparatus of claim 25, wherein the one way function f(x) is a secure hash function.

33-34. (Cancelled)

35. (Original) The apparatus of claim 25, wherein the secure information comprises a password.

36. (Original) The apparatus of claim 25, wherein the secure information comprises a key for secure communication.

37. (Original) The apparatus of claim 25, wherein the node is configured to distribute the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

38. (Original) The apparatus of claim 25, wherein the node is configured to perform the handshake process with the adjacent node once for every fixed time amount T.

39. (Original) The apparatus of claim 25, wherein the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0).

40. (Original) The apparatus of claim 25, wherein the node is configured to determine an age of the secure information so that each node in the secure group will store a latest version of the secure information.

41. (Original) The apparatus of claim 25, wherein the node is configured to check a sequence number of the secure information to determine the age of the secure information.

42. (Original) The apparatus of claim 25, wherein the node is configured to check a date of modification of the secure information to determine the age of the secure information.

43. (Original) The apparatus of claim 25, wherein the node is configured to check an elapsed time since a previous modification of the secure information to determine the age of the secure information.

44. (Original) The apparatus of claim 25, wherein the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value.

45. (Previously Presented) The apparatus of claim 25, wherein the node is configured to increase a security of the secure group by widening the key value which is known by each node in the secure group.

46. (Original) The apparatus of claim 25, wherein the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

47. (Original) The apparatus of claim 25, wherein the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every

amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

48. (Original) The apparatus of claim 25, wherein the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

49. (Previously Presented) An apparatus for secure information distribution between nodes, the apparatus comprising:

means for performing a handshake process between a first node and an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the key value associated with the secure group, to a one way function f(x); and

means for distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

50. (Previously Presented) An article of manufacture, comprising:

a machine-readable non-transitory storage medium having stored thereon instructions to:

perform a handshake process between a first node and an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to

calculate identical values by applying a component value A1 provided by the first node, a component value B1 provided by the adjacent node, and the key value associated with the secure group, to a one way function f(x); and

distribute secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

51. (Previously Presented) The method of claim 1, wherein the handshake process further comprises:

transmitting the calculated value between the first node and the adjacent node.

52. (Previously Presented) The method of claim 1,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

53. (Previously Presented) The apparatus of claim 25, wherein the handshake process further comprises:

transmitting the calculated value between the node and the adjacent node.

54. (Previously Presented) The apparatus of claim 25,

wherein the node belongs to the secure group if the node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

55. (Previously Presented) The apparatus of claim 49, wherein the handshake process further comprises:

transmitting the calculated value between the first node and the adjacent node.

56. (Previously Presented) The apparatus of claim 49,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

57. (Previously Presented) The article of manufacture of claim 50, wherein the handshake process further comprises:

transmitting the calculated value between the first node and the adjacent node.

58. (Previously Presented) The article of manufacture of claim 50,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.